PTOL-413A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 09/448,854 First Named Applicant: BARBARA L. FOX
Examiner: ZAND, KAMBIZ Art Unit: 2132 Status of Application: UNDER EXAMINATION

Tentative Participants:
(1) KAMBIZ ZAND (2) KENNETH PALEY

(3)_____ (4)_____

Proposed Date of Interview: 3/2/04 **Proposed Time:** 5:30 (AM)(PM)

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description:_____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rej	1, 14, 23, 29, 35	US PAT# 6,230,266	[✓]	[ ]	[✓]
(2)_____	_____	_____	[ ]	[ ]	[ ]
(3)_____	_____	_____	[ ]	[ ]	[ ]
(4)_____	_____	_____	[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Arguments to be Presented:
EACH CLAIM HAS AT LEAST 2 ELEMENT NOT DESCRIBED IN THE PRIOR ART

An interview was conducted on the above-identified application on 03/02/04.

NOTE:
This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

Kurt Paley
(Applicant/Applicant's Representative Signature)

(Examiner/SPE Signature)

LAW OFFICES OF ALBERT MICHALIK, PLLC
704 228TH AVE NE
SAMMAMISH, WA 98074

COVER

TO: EXAMINER KAMBIZ ZAND
United States Patent and Trademark Office
Group Art Unit 2132
Telephone: 703-306-4169
Facsimile: 703-746-5457

FROM: KENNETH PALEY
LAW OFFICES OF ALBERT MICHALIK, PLLC
206-527-6637

5 Pages consisting of "APPLICANT INITIATED INTERVIEW" (4 pages) and "Applicant Initiated Interview Request Form (1 page), plus cover

Date: February 27, 2004
Subject: App. #. 09/448,854

In re Application of: Fox et al
Application Serial No. 09/448,854
Attorney Docket No.: 1850
Group Art Unit:: 2132
Examiner: Zand, Kambiz
Filing Date: 11/23/99
For: Certificate Reissuance For Checking The Status Of A Certificate In Financial Transactions

February 27, 2004

Via fax to Examiner Kambiz Zand
Tel. # 703-306-4169

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPLICANT INITIATED INTERVIEW

Applicant's representative, Kenneth Paley, of the Law Offices of Albert S. Michalik, wishes an interview with the Examiner, currently scheduled for March 2, 2004, at 5:30 PM EST, to discuss the Perlman reference (US Patent No. 6,230,266) as it relates to Applicants' Application, particularly the §102 rejection of Applicants' independent claims, in particular:

Claim 1 which may be amended to read:
1. (currently amended): A computer-readable medium having computer-executable instructions, comprising:
receiving a first transaction request in association with a first certificate issued by a certificate authority, the first certificate having a representation of an issuer name and a subject name;
communicating with a status authority to query for current status information on the first certificate; and
receiving a second certificate from the status authority indicating the current status of the first certificate, the second certificate having a representation of the issuer name and the subject name.

Claim 14 which may be amended to read:
14. (currently amended): A computer-readable medium having computer-executable instructions, comprising:
receiving a query from a relying party for current status information on a first certificate, the first certificate having a representation of an issuer name and a subject name; and
issuing a data structure including a second certificate indicating the current status of the first certificate, the second certificate having a representation of the issuer name and the subject name.

Claim 23 which may be amended to read:

23. (currently amended): A method for performing electronic commerce, comprising,

receiving, at a certificate authority, a first request for a certificate;

verifying whether the certificate should be issued, and if so, issuing the certificate;

receiving a second request at a status authority for status information about the certificate; and

issuing a reissue certificate including the status information in response to the receiving a second request at a status authority for status information about the certificate.

Claim 29 which may be amended to read:

29. (currently amended): A method for performing electronic commerce, comprising:

receiving a certificate at an end entity;

providing the certificate to a relying party; and

receiving a receipt at the end entity from the relying party, the receipt including a reissue ~~status information about the~~ certificate.

And Claim 35:

35. (original): A method for performing electronic commerce, comprising,

receiving a certificate with a request to perform a transaction;

communicating with a status authority to request status information about the certificate;

receiving a reissue certificate including the status information in response to the request; and

deciding whether to perform the transaction based on the status information.

In general terms, Applicants understand that Perlman describes a scheme for delegation and revocation (renunciation) of a certificate authority's authority to revoke a certificate that it has issued to a network of online revocation servers. Perlman describes two types of certificates for this purpose, a delegation certificate and renunciation certificate.

In the described Perlman embodiment (FIG. 2), a system includes a plural quantity of certificate authority (CA) and associated on-line revocation server (OLRS) pairs. Principals (nodes) request a CA to issue certificates to authenticate their public keys, and the CA issues such certificates (Col. 5, lines 43-45). The CA is informed which unexpired certificates should no longer be honored (Col. 5, line 47). The CA stores revoked certificates in a master

Certificate Revocation List (CRL) (Col. 5, lines 48-49). The OLRS obtains via unspecified means the information contained in the CA's master CRL, and may augment the master CRL via unspecified means with real-time additional CA issued unexpired revoked certificates (Col. 5, lines 59-68). The OLRS's master CRL and the real-time information together form certificate revocation status information available to inquiring principals (Col. 5, lines 65-67). The OLRS provides to a verifying principal this certificate revocation information (Col. 5, lines 56-57). A verifying principal may query the OLRS for the stored certificate revocation status information, to determine whether a particular query specified certificate has been revoked (Col. 6, lines 1-4). The OLRS authenticates the result of a particular query by signing the result using its private key (or by a secret negotiated session key) (Col. 6, lines 4-8). The OLRS may also provide to inquiring principals certificates indicating whether the particular certificates specified in the query have been revoked, and/or the delegation certificate provided to it by the CA authorizing the OLRS to provide certificate revocation status information (Col. 6, lines 8-13).

If the CA determines that the OLRS has been compromised, a second (i.e., uncompromised) OLRS 206 having substantially the same configuration and operation as the first OLRS, is made part of the system along with its paired CA. (Col. 6, lines 23-29)

Assuming that the CA has not been compromised, the second CA generates, after compromise of the OLRS is detected, a special delegation certificate for the second OLRS, that authorizes the second OLRS to provide certificate revocation status information on behalf of the second CA, signs the special delegation certificate using the private key belonging to the second CA, and supplies the signed delegation certificate to the second OLRS and/or network directory service (Col. 6, lines 30-42). After verifying that the special delegation certificate is properly signed by the second CA , the second OLRS begins to supply certificate revocation status information and copies of the special delegation certificate to verifying principals (Col. 6, lines 42-46). Alternatively, if the second OLRS is unable to verify that the special delegation certificate is properly signed by the second CA, the delegation certificate is ignored (Col. 6, lines 46-49).

The special information contained in the special delegation certificate notifies verifying principals furnished with the delegation certificate that certificates issued by the first CA, except the delegation certificate authorizing compromised first OLRS to provide certificate

revocation status information on behalf of the first CA, should continue to be honored as valid, but that all inquiries regarding revocation of certificates issued by the second CA should be directed to the uncompromised second OLRS, as the first OLRS has been compromised (Col. 6, lines 50-59).

The remainder of Perlman generally describes schema for determining whether an OLRS has been compromised, and if so having another OLRS paired with a different CA provide revocation status to inquiring principals. Perlman's certificates are issued to the public key of the OLRS (as illustrated in the figures.) There is no description of a mechanism for an OLRS being sent such a certificate. When an OLRS gives status, it presumably signs the status and includes its own delegation certificate. There is nothing in Perlman that indicates that the OLRS always issues a new certificate. If all an OLRS obtains in a query is a serial number, it is only an assumption that an OLRS pulls a public key from a certificate and signs it as a response.

Respectfully submitted,

Kenneth Paley, Registration No. 38,989
Attorney for Applicant
Law Offices of Albert S. Michalik, PLLC
704 - 228th Avenue NE
Sammamish, WA 98074
206-527-6637